UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/776,416	02/11/2004	Yannick Teglia	S1022.81102US00	2402

23628 7590 04/06/2007
WOLF GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
DARE, RYAN A	
ART UNIT	PAPER NUMBER
2186	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/776,416	TEGLIA, YANNICK	
	Examiner	Art Unit	
	Ryan Dare	2186	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,9-12,17 and 18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,9-12,17 and 18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 1-6, 9-12 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sato et al., US Patent 5,734,855, in view of Philipp, DE19936890.

4. With respect to claim 1, Sato et al. teach an integrated circuit implementing at least one operator, and functionally comprising upstream and downstream of the operator at least one source register and at least one destination register, respectively, at least one temporary register to store a content of the source register or a result of the operator before transfer to the destination register, in col. 2, lines 24-57. However, Sato et al. fails to disclose loading a random number into the destination register. Philipp teaches that in order to keep a secret quantity secret from cryptanalysis or observation,

to load a random or pseudo random number at least into the destination register, in the Abstract, thus curing the deficiencies of Sato et al.

5. It would have been obvious to one of ordinary skill in the art having the teachings of Sato and Philipp before him at the time the invention was made to modify the memory system of Sato with the memory system of Philipp in order to load a random number into the resultant register in order to thwart a potential enemy eavesdropping on the register through cryptanalysis by observation of the register, as taught by Philipp in the abstract.

6. With respect to claim 2, Philipp teaches the circuit of claim 1, wherein said random number is loaded into the destination register before transfer of a result of the operator to this register, in the abstract.

7. With respect to claim 3, Philipp teaches the circuit of claim 1, further comprising means for loading the temporary register with a random quantity, in the abstract. Since the temporary register stores the result of the operation, as does the destination register, it would be obvious to write the secret quantity into the temporary register as well, for the reasons listed above in the rejection of claim 1.

8. With respect to claim 4, Philipp teaches an antifraud method comprising randomizing a content of a destination register of a result of an operator involving at least one secret quantity, and inputting a random quantity in the destination register before each loading of a result therein, in the Abstract. Philipp fails to teach loading the result of the operator being into a temporary register before loading into the destination register. Sato teaches loading the result of the operator being into a temporary register

before loading into the destination register in col. 2, lines 24-57, thus curing the deficiencies of Philipp.

9. It would have been obvious to one of ordinary skill in the art having the teachings of Sato and Philipp before him at the time the invention was made to modify the memory system of Sato with the memory system of Philipp in order to load a random number into the resultant register in order to thwart a potential enemy eavesdropping on the register through cryptanalysis by observation of the register, as taught by Philipp in the abstract.

10. With respect to claim 5, Philipp teaches the method of claim 4, wherein the integrated circuit comprises at least one operator involving at least one secret quantity, and means for loading a random or pseudo-random number at least into the destination register, in the Abstract. Sato teaches functionally comprising upstream and downstream of the operator at least one source register and at least one destination register, in col. 2, lines 24-57.

11. With respect to claim 6, Sato teaches an integrated circuit comprising: an operator; a destination register coupled to receive a result of the operation, a source register coupled to provide data to the operator; and a temporary register configured to store the data of the source register or the result of the operation, in col. 2, lines 24-57.

Sato fails to teach loading a random number. Philipp teaches:

a control circuit configured to load a random or pseudo-random number into the destination register before transfer of the result into the destination register, to protect against attacks by physical signature analysis, in the Abstract.

Although Philipp does not teach that the control circuit is configured to load a random or pseudo-random number into the temporary register, the combination of Philipp with Sato does, since with the invention of Sato, everything is transferred first to the temporary register and then to the destination register. Thus the combined invention would transfer the random value first into the temporary register and then into the destination register.

12. It would have been obvious to one of ordinary skill in the art having the teachings of Sato and Philipp before him at the time the invention was made to modify the memory system of Sato with the memory system of Philipp in order to load a random number into the temporary register and resultant register in order to thwart a potential enemy eavesdropping on the register through cryptanalysis by observation of the register, as taught by Philipp in the abstract.

13. With respect to claim 9, Sato teaches an integrated circuit as defined in claim 6, wherein the control circuit is configured to transfer the result of the operation into a temporary the temporary register and to transfer the result of the operation from the temporary register to the destination register, in col. 2, lines 24-57. Sato fails to teach loading a random or pseudo-random number into the destination register. Phillipp teaches this in the abstract.

14. With respect to claim 10, Sato teaches an integrated circuit as defined in claim 7, wherein the control circuit is configured to transfer data from the source register to the temporary register, and to transfer the result of the operation to the destination register

in col. 2, lines 24-57. . Sato fails to teach loading a random or pseudo-random number into the destination register. Phillipp teaches this in the abstract.

15. With respect to claim 11, Sato teaches an integrated circuit as defined in claim 6, wherein the destination register is a source register for a second operator, in col.13, lines 47-60.

16. With respect to claim 12, Sato teaches transferring a result of the operation into a temporary register, then into a destination register in col. 2, lines 24-57, but fails to teach randomizing the content of the temporary or destination register before transferring a result involving a secret quantity. Philipp teaches randomizing the content of the destination register to protect against attacks by physical signature analysis in the Abstract. Although Philipp does not teach that the control circuit is configured to load a random or pseudo-random number into the temporary register, the combination of Philipp with Sato does, since with the invention of Sato, everything is transferred first to the temporary register and then to the destination register. Thus the combined invention would transfer the random value first into the temporary register and then into the destination register.

17. It would have been obvious to one of ordinary skill in the art having the teachings of Sato and Philipp before him at the time the invention was made to modify the memory system of Sato with the memory system of Philipp in order to load a random number into the resultant register in order to thwart a potential enemy eavesdropping on the register through cryptanalysis by observation of the register, as taught by Philipp in the abstract.

18. With respect to claim 17, Applicant claims a method that corresponds to the circuit of claim 11 and is rejected using similar logic.

19. With respect to claim 18, Applicant claims a method that corresponds to claim 12 and is therefore rejected using similar logic.

Response to Arguments

20. Applicant's arguments filed 1/08/07 have been fully considered but they are not persuasive. Applicant claims that there would have been no motivation to combine Sato with Philipp since Sato does not describe a cryptographic or masking problem. However, the same motivation does not need to be found in both references. If one of ordinary skill in the art at the time the invention was made, having the invention of Sato, was presented with the problem of a cryptographic analysis adversary, the skilled artisan would have looked to the invention of Philipp to cure the deficiency. Both are memory systems dealing with loading the result of operations into registers and thus are analogous art. The examiner has clarified the above rejection to make it clear how the combination of Sato and Philipp teach all limitations of the claims as they stand currently amended.

Conclusion

21. The prior art made of record on form PTO-892 and not relied upon is considered pertinent to applicant's disclosure. Applicant is required under 37 C.F.R. § 1.111(c) to

consider these references fully when responding to this action. The documents cited therein teach similar memory systems.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ryan Dare whose telephone number is (571)272-4069. The examiner can normally be reached on Mon-Fri 9:30-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matt Kim can be reached on (571)272-4182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ryan A. Dare
April 1, 2007

PIERRE BATAILLE
PRIMARY EXAMINER
4/2/07